Declaration of standards for ethical software behavior

honeygain® {dev}

Contents:

Foreword	03
Honeygain SDK AppEsteem compliance report	04
Honeygain SDK CSA compliance report	11
Honeygain SDK Avast/AVG compliance report	20
Honeygain SDK McAffee compliance report	27
Honeygain SDK Microsoft Windows compliance report	36
Honeygain SDK Malwarebytes compliance report	42
Honeygain SDK Google compliance report	43
Honeygain SDK Avira compliance report	47

Foreword

Philosophical and practical care about the future of ethical software and the integrity of cyberspace is in the core of Honeygain SDK. We envision a software ecosystem founded on trust and transparency. One that promotes sustainable, consumer-friendly practices across the industry and this vision is not simply idealistic - it's practical and necessary. Trustworthy and transparent software fosters a safer digital world where users can engage with apps based on new business models without fear. By upholding high standards of integrity now, we lay the groundwork for a more trustworthy and open ecosystem in the years to come.

Hybrid monetization, a domain that has historically been a gray zone is an area where clear standards are especially needed as it has often lacked explicit guidelines. Without well-defined standards, even well-intentioned developers risked blurring the line between innovative monetization and exploitative practices. In this declaration, we address that gap by establishing transparent rules for how our software works while earning revenue. ***We must emphasize that our SDK is an addition to a standalone app managed by those who choose to integrate with us and pass our screening.*** *Our SDK by fundamental means cannot execute such operations as advertising or collection of valuable personal user data. By bringing full clarity to how our product make money, we seek to eliminate surprises and build partner and user confidence.*

It's important to note that compliance to the following requirements did not came overnight. This declaration is the result of humbling internal evaluation of our own practices, measured and put against the best external benchmarks. In developing our standards, we drew upon principles set by leading security and platform organizations - from AppEsteem and the Clean Software Alliance to guidelines set by companies like Google, Microsoft, Avast, Malwarebytes, and Bitdefender and alike. We actively benchmarked our processes to these industry standards to ensure that our commitment meet our end goal: to build software that genuinely benefits users, developers, and platforms alike. We believe that by holding ourselves accountable, we set stage to create a positive-sum ecosystem where users are respected and safe, legitimate developers thrive, and platforms maintain their integrity.

The Honeygain SDK team

Honeygain SDK AppEsteem compliance report

1. TRANSPARENCY & HONEST COMMUNICATION

ACR ID	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
ACR-003	Consumers are not misled to believe they have an issue, a problem with, something out of date, or something missing from their system. This includes no exaggerated or unsubstantiated claims about system's health. This requirement is to ensure that the consumer isn't scared or tricked into taking action, especially paying for something not available in a fully functioning trial. Example violation: a free scan shows consumers errors/problems with registry settings, but only fixes after consumer pays. The solutions: tone down the scan results to reflect reality, or provide a fully functional free trial.	✅
ACR-004	When showing free scan results with the intent to monetize, results are substantiated and avoid any exaggerated sense of urgency, and app provides free fixes, either during an immediate, fully functional free trial of at least 24 hours for all free scan results shown, or when the fix is not anticipated to be permanent. Free trial does not pre-collect payment details or use negative options to charge consumer unless free trial is an immediate, fully-functional trial lasting at least seven days. Because they offer hard-to-verify services at a vulnerable time for a consumer, System Utilities must take great care to avoid any sense of coercing the consumer to take action when they provide free scans, especially without immediate fully functional free trials.	✅
ACR-005	Does not impersonate or mimic a system, browser, or component message or prompt. The intent is that consumers can distinguish advertising, monetization, and app messages from the platform and browser messages and prompts.	✅
ACR-006	All value propositions, including any alternative monetization ones (e.g., search, advertising, and affiliate links), are accurately and equitably disclosed, attributed, and available in the app's name, offer, install, and software. The intent is that consumers are aware of all value propositions and monetization approaches of an app, and that these were equally disclosed to them.	✅
ACR-007	Has no false claims or implications to be from another vendor or misleading users about their source, owner, purpose, functionality/ features. Provides explicit notification to all affected parties and obtains informed user consent when reducing the default capability of, or moving away from certified versions of, security or safety. The intent is that consumers don't think they're clicking/accepting/installing/taking action on a different vendor's app or system, and that they are aware when their security or safety posture will be lower that the default of the system or the brand.	✅
ACR-008	If app must provide free fixes to free scan results, the details regarding the free fix must be obvious, mentioned within the app itself, not solely part of a purchase flow, available simultaneously with a purchase flow, and no more difficult to obtain than the fully functional version. The intent is that consumers can find the free options in the software as easily as they can find the purchase option.	N/A - No scan
ACR-009	Has no threatening messaging. Consumers must not be coerced into taking action.	✅

- **Based on AppEsteem requirements:** customer.appesteem.com/home/checklist?minbar=y

ACR ID	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
ACR-014	Is truthful and not misleading or confusing with the intent to deceive; can be substantiated; is not unfair. Consumers aren't surprised or tricked by where the ad takes them or what the app claims	✅
ACR-017	Certifications, representations, and endorsements are not false, misleading, or fraudulent. Consumers have a right to not be unpleasantly surprised because they thought the app came from or was recommended by some other source. This includes implied certifications and endorsements that don't apply to the app; it must be clear as to what specifically was endorsed or certified. Expired certifications must also be removed or specific as to the timeframe.	✅

2. ADVERTISING & MONETIZATION ETHICS

ACR-016	Downloads are not launched directly from advertisements. Ads lead to offers, not directly to downloads.	✅
ACR-020	Easily distinguishable from the web site's existing ads and web site content. Injected ads must be identifiable as injected and not part of the website	✅
ACR-024	Honors the relevant passed-through platform policies and terms of use for advertising, content, and search advertising. Injectors have an obligation to honor a platform's desires. Injected ads must honor appropriate platform policies.	✅
ACR-025	Injects no more than one interstitial ad, one non-interstitial ad, five hyperlink-based ads, and one search box per page. The intent is that ad injectors must limit how much they change the consumers' expected experience.	✅
ACR-030	Consumer can navigate away from interstitials (and interstitial will close), including at a minimum a close button. If the interstitial restricts access to publisher content, then the consumer must be able to use the back button, the address bar, and clicking outside the ad or offer as methods to close the interstitial. The intent is to not force the consumer to choose or interact before proceeding with their intention.	✅
ACR-031	Interstitials are not chained together. One interstitial only can be injected. One interstitial offer can be added to a landing page.	✅
ACR-032	Shown only after the consumer clicks to do something besides exiting the page. If interstitial displays in a different window or tab, shown only after a positive user action. Except when they're in the same window and tab, interstitials must be tied to positive and intentional user actions.	✅
ACR-046	Disclosures and options are conspicuous and visible without requiring scrolling or other user actions. The method to enable and disable options is clear and conspicuous. The intent is that the consumer can see everything on one easy-to-read, easy-to-access, screen.	✅

ACR ID	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
2. ADVERTISING & MONETIZATION ETHICS		
ACR-110	Does not hijack existing monetization relationships by cookie stuffing, replacing hyperlinks, replacing ads, or other related techniques. Intent is that app should not divert others' paid efforts or relationships.	✅
ACR-155	Ads and offers are not inserted to masquerade as part of existing committed user workflows. Intent: no tricking the consumer into thinking this is the normal flow once the consumer commits to download/ purchase/accept/uninstall. For instance: an interstitial offer on another app's landing page must not look like it's part of the other app's download or install flow, and an interstitial ad should not look like it's part of a consumer purchase.	✅
3. USER CONSENT & CONTROL		
ACR-039	Everything installed per app, especially other apps, offers, and download managers, has clear indications of the relationship to the app. Consumers must be able to understand the relationship within the files and with other apps. This should be accomplished in EULAs, readme files, how the files and directories are named, and installation location.	✅
ACR-042	No other apps or unrelated components are installed or used before obtaining the consumer's permission through explicit user action. Installs must only come after consumer-accepted offers.	✅
ACR-043	Nothing is installed that was not disclosed. Anything installed, even if not enabled by default, must be disclosed in the offer and in the docs. This includes third party components, and components digitally signed by other parties.	✅
ACR-047	Does not deceive or mislead consumers to take any action that they previously declined or cancelled. No means no. Consumers must not be misled to restart a cancelled installation or declined offer.	✅
ACR-048	Does not hide and/or limit the consumer's ability to close, delete, disable, or uninstall the app.	✅
ACR-050	User consent dialogs and feature settings from the browser, search, or operating system, and existing security/safety apps, are not circumvented or blocked. Does not ask for more than the minimum permissions necessary to fulfill its offered value proposition.	✅
ACR-051	Uses available APIs to change browser settings and behaviors. If no API is available, browser is not extensible. Browsers have their own ways of managing extensibility and settings and obtaining user consent. Apps must honor those ways.	✅

ACR ID	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	3. USER CONSENT & CONTROL	
ACR-053	If more than two offers will made before, during, or after install, all but the final offer has a "skip offers" option. The intent is the user can stop a long offer flow chain.	✅
ACR-055	Accept, cancel, skip, and decline options are obvious and/or explained to the consumer, consistently simple, and consistent across the install and offer experiences. No attempting to mislead, shortcut, or even "guilt" the consumer. For instance, don't say "No, I don't want friends" on the decline button. Declines and skips must be no more difficult to perform than accepts. Also, bundlers can't have the buttons work differently for different offers.	✅
ACR-057	Provides a clear way for consumers to accept or decline. Offers need to be straightforward and open about how to accept or reject the offer.	✅
ACR-059	Clearly marked as an offer, clearly implies it is optional, and only claims to be recommended when the recommender is explicitly disclosed. Offers need to be recognizable as offers. Recommendations must be claimed by whoever is making them.	✅
ACR-060	Discloses any applicable third-party offer provider. Consumers need clarity on who is responsible for the offer and verifying that it is legitimate and trustworthy.	✅
ACR-071	Each offer must be able to be accepted or declined independently. The intent is that consumers aren't forced to accept bundles of offers and "free bonuses" in the shopping cart	✅
ACR-075	No apps are installed, and no more apps are offered, when the consumer cancels or declines the carrier, or the carrier install fails. Cancellation by the consumer, or carrier install failure, means nothing at all gets installed: no carrier, no offered apps, no settings changes.	✅
ACR-109	Only downloads and/or installs apps that the consumer chose and agreed to install. Consumers get to choose what gets installed. No "bonuses"	✅
ACR-111	Has given clear notification and obtained explicit, informed user consent for modifying or manipulating webpage content and redirecting web traffic. Since this affects a consumer's experience with web pages, content/ad injection, blocking, and manipulation is only allowed with direct user consent about this behavior.	✅
ACR-168	If additional offers may be made to the consumer as a result of one-to-one interactions, this must be clearly and simply disclosed alongside the interaction option. One-to-one interaction options for app purchase and app feature activation must have corresponding non-interactive options that are no less prominent than the interactive options. Consumers should not be surprised when they are offered additional things when calling for support, refunds, cancellation, purchase, or activation. Consumers must have non-interactive means to purchase or activate features in their app. Equal prominence means equal real estate, displayed side by side, equal-sized font and placement, with no visual cues to influence the interactive option choice. Note that this applies to post-purchase pages as well.	✅

ACR ID	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	4. INSTALLATION & UNINSTALLATION INTEGRITY	
ACR-084	Does not attempt to hide or disguise its presence or whether it is active. Consumers have a right to know what is running on their systems.	✅
ACR-083	App updates do not install or uninstall other apps and unrelated components without explicit offers following these requirements. Updates must not become a means to avoid following the offer requirements.	✅
ACR-114	If injecting, provides a standard uninstall method for the app using the same name as shown in the ads it produces. Note that ads must meet the injected ads requirements.	✅
ACR-116	Can be uninstalled by platform standard features (e.g., operating system's or browsers uninstall and disable features). Consumers are trained by platforms on how to disable and uninstall. Apps must support these methods.	✅
ACR-117	Does not engage in any deceptive behaviors to deter uninstallation. Some examples of bad behavior: making false or misleading claims about potential negative effects, suggesting uninstallation is complete when it is not, charging fees to uninstall, making uninstallation conditional on downloading or installing other apps, making the default option to be anything other than uninstall.	✅
ACR-118	Does not install, retain, or reinstall any apps or executables without user consent during the uninstall process. Leaving executables on the system requires user consent.	✅
ACR-119	Functionally removes all monetization components of the app. The intent is that once the consumer uninstalls the app, the monetization is gone. Vendors must not monetize after uninstallation. For instance, if search was changed or affiliate IDs added, app must not leave these set when app is uninstalled.	✅
ACR-122	Once app is disabled or deleted, it isn't re-enabled by itself or another app. Apps must obey the wishes of the consumer to disable and uninstall.	✅
ACR-124	Uninstallation doesn't add unnecessary friction for the consumer. Shows no more than one uninstallation confirmation prompt with obvious and clear options presented to the consumer to continue with the uninstallation or keep the product, and no more than one suggested substitution app. The consumer must be able to perform the uninstall quickly and efficiently.	✅

ACR ID	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
5. SECURITY & DATA PROTECTION		
ACR-010	Is not malicious and does not propagate viruses, worms, trojans, Deceptors, or the like. A bundler, the app, its ads, and its offers/landing pages must take care not to become a vector for malware or Deceptors.	✅
ACR-085	Does not collect, handle, or transmit sensitive information such as banking details without proper encryption and user consent from all affected parties. Vendors have an obligation to protect consumer data. If the data is sensitive enough to require encryption, it is important enough to require direct user consent from anybody affected.	✅
ACR-086	Does not hide from any affected consumers how it collects, stores, or transmits their user activities, and to whom it provides user data. The intent is apps do not steal information from unsuspecting users of a computer. For instance, an app shouldn't collect entered URLs or typed passwords unless this is the stated purpose of the app and was disclosed in the value prop.	✅
ACR-089	Does not automatically or unexpectedly send spam, make calls, or click on ads and links. The intent is to not take actions that emulate consumer behavior in undesirable ways.	✅
ACR-097	App does not attempt to evade security investigation or detection, and does not attempt to hide or cloak the software's behavior. Looking for security products and then changing behavior is not allowed. Even the intent to change or cloak behavior is not allowed.	✅
ACR-107	Obtained proper authorization from the carrier, the offers, the ads, and any third party components included. The intent is that apps install only authorized apps and components, honor vendor takedown notices, and either have direct authorization/licensing/partnerships or honor vendor restrictions placed on padsites.org or in licenses.	✅
6. PRODUCT VALUE & FUNCTIONALITY		
ACR-103	App has an accessible primary function and a value proposition that can be verified, and that goes beyond launching another app, theme, extension, search, or web page. Apps must have their own intrinsic value that is easily accessible by the consumer.	✅
ACR-104	Does not change or offer other search providers, or redirect and/or block searches, queries, user-entered URLs, and/or access to other sites unless this functionality is the value proposition of the app, and the app provided the consumer with clear notification and attribution. Taking these kinds of actions are allowed only when these actions are one of the main reasons why the consumer is installing the app.	✅

ACR ID	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
ACR-013	User-committed acquisition workflows are not interrupted with out-of-context, non-essential, or unrelated interstitials that require the user to wait or respond, unless app has first obtained explicit, informed user consent immediately prior to the interruption. Unless they've explicitly given their informed consent immediately prior, consumers should not have to wait for or respond to extraneous questions, offers, or ads during committed workflows (downloads, installs, updates, purchases, and uninstalls).	✅

7. BILLING & TRIAL PRACTICES

ACR-164	If receiving consumer payment/billing information, consumers are notified, and are informed at signup time how and when they will be notified, of the expiration of time-bound discounts, trial periods, or other negative options and how they can opt out. The intent is to remind the consumer what they purchased when they provide their payment details, and also once the benefit of the negative offer ends. Note that opt-out methods must conform to requirements on one-to-one interactions.	✅
ACR-165	If offering time-bound discounts, trial period, or other negative options, discloses clear and simple material terms before receiving consumer payment/billing information, obtains consent before charging, and offers simple online methods to stop recurring charges. App cannot claim it is free if payment details are collected in advance. Any negative offer must be clear to the consumer about all the conditions before the transaction is completed. The intent is to align with ROSCA, a US law governing Internet negative option sales. Apps must comply to ROSCA if they offer any negative options, as defined by the FTC's Telemarketing Sale Rule.	✅

Honeygain SDK CSA compliance report

1. ADVERTISING

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
→ 01. MISLEADING ADS		
	Advertisements must not use threatening messaging.	✅ N/A - No advertising
	Advertisements must not mislead users to believe they need something that is missing from their computer.	✅ N/A - No advertising
	Advertisements must not mislead users to believe they have an issue or problem with their system (including misleading messaging that they need to update a program).	✅ N/A - No advertising
	Advertisements must not impersonate a system message or component.	✅ N/A - No advertising
	Advertisements must be distinguishable from the underlying web page and any associated call to action must clearly be attributed to the ad and not the page.	✅ N/A - No advertising
	Advertisements must not falsely or misleadingly use trust marks, company logos, or certification marks.	✅ N/A - No advertising
	Advertisements must not falsely claim to be for a program from another vendor or mislead users about their source, owner, purpose, or functionality/features (for example, claiming to be a program from Adobe, Microsoft, or Google when they are not).	✅ N/A - No advertising
	Advertisers must only market programs that they are authorized to market.	✅ N/A - No advertising
→ 02. DIRECT DOWNLOAD / AUTO DOWNLOAD		
	A product download may only be invoked by a user click on a Landing Page or Offer Screen.	✅ N/A - No advertising
	A product download must not be directly invoked from an advertisement.	✅ N/A - No advertising
	A product download must not be automatically invoked.	✅ N/A - No advertising

• **Based on CSA guidelines:** www.cleansoftware.net/guidelines

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
→ 03. LANDING PAGE	A Carrier Product must have a Landing Page that clearly explains what the Product is — including its name, key functionality, main effects on the user's computer, and whether it is ad supported.	✅ N/A - No advertising
	A Product's Landing Page must identify the Carrier Product Source and include links to the Product's EULA, Privacy Policy, and uninstallation instructions. The EULA and Privacy Policy must include up-to-date contact information for the Product Source.	✅ N/A - No advertising

2. INSTALLATION PROCESS

→ 01. USER CONSENT, CONTROL, TRANSPARENCY	Prior to installation, each Software Product must disclose, either on the Landing Page or Offer Screen: (a) the Product's name, (b) the Product Source, (c) the Product's key features and functionality — including any system or browser settings impacted, and whether the Product is ad-supported; and (d) links to the Product's EULA and Privacy Policy, along with assent language signifying user agreement.	✅
	Any disclosures required by these Guidelines must be visible without requiring additional user action (e.g., not hidden behind "Custom" or "Advanced" install options).	✅
	Opt-in or opt-out controls, as well as decline options, must not be displayed as inactive or misleading (e.g., grayed out). Landing Pages do not require a decline mechanism if users can freely navigate away.	✅
	The adequacy of disclosures is determined by considering the totality of the Landing page and/or Offer Screen. Otherwise adequate disclosures may be deemed insufficient when viewed together, for example, if font size, font color, background color, or design and/or graphical or other design elements adversely impact the display of the required disclosure(s).	✅
	Each Product must obtain End User consent before downloading and/or installing; an installer may only install Products or services that the End User chooses and agrees to install.	✅
	If a Product collects or transmits Sensitive Information, that fact must be clearly disclosed to the End User in the offer screen and consented to by the End User. The specific types of Sensitive Information being collected or transmitted, as well as an explanation of how the Sensitive Information may be used, must be described in the Product's Privacy Policy.	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	All disclosure and consent clauses should be presented to users in a clear and conspicuous manner that is easy to read and understand, and without the need for the user to click on an “Advanced” or “Custom” option.	✅
	Cancel and decline options must be obvious and/or explained to the user within the Offer Screen. If a user decides to cancel the installation process before the final offer for a Bundled Product has been made and the Carrier Product begins its installation, such cancellation should cancel the install execution of all Software Products within the Software Bundle.	✅
	If an installer’s installation process is canceled by the user, the installer must not place shortcuts to continue the installation later on the user’s PC.	✅
	Any Product with material functionality embedded from a third party must disclose and describe such functionality in the Product’s EULA and/or Privacy Policy, as applicable.	✅
	A Product must disclose to the user if and how it may affect any other programs or settings on the user’s device either in the Landing Page or Offer Screen, as appropriate depending on Product type, or otherwise in advance of the event impacting the other program(s) or settings.	✅
→ 02. MISLEADING BEHAVIORS		
	The installation of a Product must not be initiated based on false, misleading, or fraudulent representation.	✅
	Any disclosures required by these Guidelines (including those for features and settings changes) must be displayed without the user having to take any other action (i.e., no hiding disclosures behind “Custom” or “Advanced” install options, etc.).	✅
	A Product’s features and functionalities must match the description presented on the Landing Page and/or Offer Screen.	✅
	The language used during installation must not be confusing to the user (for example, double negative questions to confuse opt-out with opt-in).	✅
	A Product and its installer must not act differently in the presence of anti-malware software or anti-malware environments or virtual machine environments for the purpose of evading investigation or detection. The modification of Product or installer behaviors for the purpose of avoiding investigation or detection by other companies, browsers, or platforms is expressly forbidden.	✅
	Software must be installed in a location where the user can expect to find software installations in a manner which clearly identifies the Product, Product Source (e.g. %PROGRAMFILES%\), as well as the actual install date.	✅
	Existing program shortcuts cannot be altered or replaced by other programs and/or installers.	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
→ 03. SIGNING SOFTWARE		
	Each Installer, Product, and Product Update must be signed by its respective Product Source.	✅
	Each signature must clearly and transparently identify the entity that signed the component. The entity name must be disclosed to CSA.	✅ Honeygain SDK signature clearly and transparently identifies the entity that signed the component.
→ 04. BUNDLING SOFTWARE		
	All disclosure requirements in these Guidelines apply equally to Carrier Products and Bundled Products.	✅ N/A - No bundled software
	All Products within a Software Bundle must be disclosed on an offer screen, conspicuous to the user before acceptance without requiring excessive scrolling or accessing “custom” or “advanced” install options.	✅ N/A - No bundled software
	Each Product within a Software Bundle must be accepted independently.	✅ N/A - No bundled software
	No Product may be installed that has not been disclosed on an Offer Screen in accordance with these Guidelines.	✅ N/A - No bundled software
	The same Bundled Product may not be offered more than once in the same bundle.	✅ N/A - No bundled software
	Each Offer Screen should provide users with a clear way to accept or decline the offer.	✅ N/A - No bundled software
	The presentation of the accept and decline options within an Offer Screen shall be of equal prominence.	✅ N/A - No bundled software
	An Offer Screen must have the brand of the Product offered; any Carrier or third-party logos must not mislead the user.	✅ N/A - No bundled software
	If the bundle has more than one Bundled Product, there must be a ‘skip all’ option on all Bundled Product offer screens, except the final offer screen.	✅ N/A - No bundled software
	Each Bundled Product should be clearly marked as optional and/or promoted content (e.g., Promotional offer, Optional offer, Advertisement, Promoted content).	✅ N/A - No bundled software
	The name of the Product shown in the Offer Screen must match the product name in the OS and browser libraries and removal dialogs.	✅ N/A - No bundled software
	When the user cancels or declines to install the Carrier Product, the installer should end without offering any Bundled Product(s).	✅ N/A - No bundled software

03. GENERAL PROGRAM FUNCTIONALITY

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
→01. PRODUCT BEHAVIOR	Products must not hide and/or limit the user's ability to close, delete, disable or uninstall the program.	✅
	Products must not install, reinstall, uninstall or remove third-party software without the user's consent, except in the case of a bona fide anti-virus/security Product acting in a security/user protection capacity or where such behavior is integral to the functionality of the Product (for example, in the case of utilities such as driver/product updaters).	✅
	Products must not hide or disable other programs without user consent.	✅
	Products must not modify third-party programs without user consent.	✅
	Products must not modify system or browser settings without clear disclosure and user consent.	✅
	A Product must not attempt to hide or disguise its presence or operation; except for legitimate background processes, a Product must not fail to clearly indicate when the program is active.	✅
	Products must meet user expectations that system maintenance or optimization actions are actually beneficial.	✅
	A Product's actual functionalities must comport with the disclosures and description provided in the Landing Page and Offer Screen.	✅
	Products must include a copy of or link to the applicable EULA and Privacy Policy; the EULA must include the name of the Product and the identity of, and contact information for, the Product Source.	✅
→02. MISLIEADING BEHAVIORS	Products must not falsely claim to be a program from another vendor, must not mislead users about their source, owner, purpose, functionality/ features (for example, claiming to be a program from Adobe, Microsoft, or Google when they are not).	✅
	Products must not alter or replace existing shortcuts.	✅
	Products may not use misleading branding (icons, names, etc.) to confuse users (for example, a Chromium browser must use a distinctly different icon from Chrome and may not call itself Chrome).	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
→02. MISLIEADING BEHAVIORS		
	Products must not display misleading or exaggerated claims about the system's health, such as make misleading or inaccurate claims about files, registry entries, the danger of leaving an identified issue as-is, or other items on the system.	✅
	Products must not deceive or mislead users to take any action that the user has previously declined.	✅ Honeygain SDK never misleads users or prompts actions that were previously declined.
→03. PROHIBITED PRODUCTS		
	Products must not be malicious or contain viruses, worms, trojans, or the like.	✅
	Products must not be designed for the purpose of engaging in activity that violates any applicable law.	✅
→04. UPDATE		
	A Product's updater can only update the original Product and may not install or uninstall other products or other unrelated components as part of the update without an explicit offer affording proper disclosure and user consent.	✅
	A Product's updater must not materially change the Product's functionality from what was described during the original installation without proper disclosure and user consent. For the avoidance of doubt, the addition or removal of a key feature or functionality (i.e., a feature or functionality disclosed in the offer screen for the Product), or the change to any system or browser setting shall constitute a material change.	✅
→05. SECURITY COMPLIANT BEHAVIOR		
	Products must neither act maliciously, nor take measures to avoid and/or evade anti-malware detection or analysis.	✅
	Products will not engage with interfering, hiding, uninstalling, or disabling any third party content, application, browser functionality and/or settings, websites, widgets, the operating system, or any part thereof without user consent.	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	Except in connection with bona fide security or parental control Products used for their intended purposes, products will not subvert security settings or protocols (e.g. SSL) for any purpose..	✅
→06. BROWSERS; OPERATING SYSTEMS (THIS SECTION DESCRIBES CHANGES MADE TO BROWSERS OR OPERATING SYSTEMS)		
	Products must not change browser or system settings without explicit user consent. For example: – Browser homepage, start page, or new tab page. – Default search provider. – Default program settings (e.g., default browser, default media player).	✅
	When changing a setting or behavior in a Member Product browser, if there are available APIs or other methodologies documented by the Product Source of such browser to effectuate such change, a Product must utilize that API or methodology.	✅
	Products should not limit the user's ability to view or modify system settings, browser settings, or extensions either directly or by another product to which the user gave consent to change browser settings.	✅
	Once disabled, programmatic re-enablement of a disabled program is prohibited without disclosure and user consent.	✅
	Products must not redirect or block searches, queries, URLs, or site access without clear notification and attribution.	✅
→07. PROGRAM GENERATED ADVERTISING	"This section applies to advertisements that are presented on a user's machine that would not otherwise be there but for the existence of a Product. All such advertisements are the responsibility of that Product. Advertisements. All promotions must adhere to the following rules:"	
	Any ads served by a Product must be identifiable as coming from that Product and linked to its EULA/website/uninstall instructions.	✅ N/A - No advertising
	The attributed name from the advertisement must match the install/ uninstall Product name.	✅ N/A - No advertising
	Users must be able to close advertisements through obvious means.	✅ N/A - No advertising
	Ad type specifics. This section talks about some of the specific criteria for the different types of advertising.	✅ N/A - No advertising
	User Opt-Out. With respect to Products that inject into or display advertising in or on top of third-party properties, the Product Source must provide users a means to either turn off, opt-out from having specific types of advertisements displayed, or remove the Product entirely.	✅ N/A - No advertising

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	04. UNINSTALL	
	A Product must be uninstallable either via the operating system's standard install/uninstall features (e.g., Add/Remove Programs) and/or through a browser's extensions/add-on library. All Product entry data in the OS or browser add/remove settings must be accurate and complete, including Product name, Product Source, and installation date.	✅
	A Product may only show a single uninstallation confirmation prompt. Such confirmation prompt must not be misleading (including suggesting that the uninstallation is complete when it is not), nor may it leverage scare tactics to dissuade the user from uninstalling the product, nor may it introduce unnecessary friction. The options presented to the user to continue with the uninstallation or keep the product must be obvious and clear. The Product's owner may include an advertisement for a single substitute product in the confirmation prompt. Such advertisement must not interfere with the uninstallation of the original Product, and may not trigger the install of the substitute product.	✅
	Products must offer the ability to be completely removed, not just disabled.	✅
	When operating, a Product must not limit or hide user controls, making it difficult to close, delete, or uninstall the Product.	✅
	A Product's name must be disclosed by its Product Source to CSA, and be consistent across all points of user interaction so that the user can clearly identify the app they may want to uninstall. This includes, without limitation: – The Product Offer Screen or Landing Page; – The Product name displayed during the operation of the product. – The Product name in the operating system's add/remove control panel and/or browser extension library, as applicable. – The Product name displayed in the "Ads by" or similar attribution. – The code signing CN value.	✅
	Products must not install, reinstall, uninstall, or remove any software without the user's consent during the uninstall process.	✅
	GLOSSARY	
	Bundled Product: means a distinct, supplemental Product or service that is offered during the download or installation of a Carrier Product.	✅
	Carrier Product: means the primary, or marketed Product or service. (Contrast with Bundled Product which is always bundled with a Carrier Product.)	✅
	End User: means an individual user who installs and/or uses any Software Product.	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	EULA: means the end user license agreement governing an End User's use of a Product.	✅
	Landing Page: means the web page wherein a Carrier Product's key features and functionalities are disclosed and from where an End User can initiate the download and installation of said Carrier Product.	✅
	Member Product: means a Product whose Product Source is a member in good standing of the CSA.	✅
	Offer Screen(s): means any screen(s) displayed to the End User during the installation process of a Product on which details of the specific Product or an offer for a Bundled Product is presented.	✅
	Privacy Policy: means the privacy policy applicable to the relevant Software Product.	✅
	Product: means an application, plug-in, helper, component, reset technology or other executable code, including, without limitation, desktop/client applications, cloud-based applications, browser extensions and javascript. For purposes of these Guidelines, a Product may include a single item, or a combination/suite of contextually- or functionally-related items from a single Product Source.	✅
	Product Source: means, with respect to any specific Product, the owner, the sponsor, or in the case of open source, the distributor. Typically the Product Source is the entity or individual(s) responsible for actively placing the Product into the relevant channel of distribution. A Product Source must always be identified by a validly registered company name or a live, human individual's name.	✅
	Sensitive Information: means personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, and specifically includes: governmental identifiers (e.g., social security number, alien registration number, passport number); biometric identifiers; health records; banking or similar information; log-in credentials; or a comprehensive browsing or keystroke history for a particular individual.	✅
	Software Bundle: means an installation flow comprising a Carrier Product and one or more Bundled Products.	✅
	Software Products: means Carrier Products and Bundled Products.	✅
	TOS / Terms of Service: means any screen(s) displayed to the End User during the installation process of a Product on which details of the specific Product or an offer for a Bundled Product is presented.	✅

Honeygain SDK Avast/AVG compliance report

1. ADVERTISING

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
MUST HAVE		
→ 01. LANDING PAGE		
	A landing page must clearly identify the vendor, describe the software, include cost (if applicable), indicate ad-supported status, and provide accessible EULA and Privacy Policy.	✅ N/A - No advertising
	List all bundled software, third-party components or dependencies (monetization engines), plugins, or widgets.	✅ N/A - No advertising
	Include links to the product's EULA and Privacy Policy.	✅ N/A - No advertising
	All information must be presented in a readable way (no distracting colors or font sizes).	✅ N/A - No advertising
→ 02. DISCLOSURE AND CONSENT		
	All app-promoting pages must clearly identify the vendor.	✅ N/A - No advertising
PROHIBITED		
→ 01. MISLEADING ADS		
	Ads must not use threatening messages.	✅ N/A - No advertising
	All forms of deceptive behavior (i.e. missing codecs, plugins, vulnerable/ infected machine, when there is no need for such thing).	✅ N/A - No advertising
	All forms of impersonation of system messages (Windows UI, MSFT/ Windows logo...), other brands (Chrome, Flash, anti-malware...) or web components (download buttons...).	✅ N/A - No advertising

• **Based on Avast/AVG guidelines:** files.avast.com/files/viruslab/whitepapers/avast_clean_guidelines.pdf

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	Displaying multiple “calls to action” with different wording leading to similar action.	✅ N/A - No advertising
	Advertising a free product for a cost.	✅ N/A - No advertising
→ 02. DOWNLOAD		
	Product downloads must not be auto-initiated or triggered directly from ads.	✅ N/A - No advertising
→ 03. DISCLOSURE AND CONSENT		
	Do not start app download or installation without proper disclosure and user consent.	✅ N/A - No advertising

2. INSTALLATION PROCESS

RECOMMENDED:		
→ 01. SIGNING SOFTWARE		
	Every executable file must contain a vendor identifier. No specific format is required, but Version Info is preferred. A plaintext description in a custom section is also acceptable.	✅
	Digital signature is always beneficial.	✅
	If the file is packed, it should have a Taggant.	✅
MUST HAVE		
→ 01. BUNDLING SOFTWARE		
	All programs offered to users must be legitimate and provide a clear, positive value to the installing user.	✅ N/A - No bundled software
	Each program must be offered in its own offer/install screen with clear information about functionality, behavior, cost (where relevant) and purpose of the software it offers.	✅ N/A - No bundled software

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	Each offer screen must have clearly labeled skip/decline button or opt-in/ opt-out checkbox which enable the user to decline the offer.	✅ N/A - No bundled software
	Each offer screen must have the same wording, “Call to Action” buttons, navigation style and button placement through the installation process.	✅ N/A - No bundled software
	Any software that includes 3rd party components or software therein must provide appropriate disclosure to end users.	✅ N/A - No bundled software
→ 02. USER CONSENT, CONTROL AND TRANSPARENCY		
	All disclosure and consent clauses must be unavoidable to end users, must meet industry standards for readability a must be presented in a language that an ordinary end user comprehends.	✅
	User consent must be obtained before download/installation of any software.	✅
	The installer must only install the software which user provided their consent to install.	✅
	The user must be able to stop the installation at any point.	✅
	Any data acquisition shall be made under the end user’s consent.	✅
	Each setup screen must include exit functionality.	✅
	App installation must not be affected by any user decisions on the offers.	✅
	App must disclose to user name of product, identify developer name or brand name as the providing entity, how to contact such entity.	✅
	Software’s EULA must disclose to user if and how app may affect any other programs on user PC and settings.	✅
	It must be clear in which stage the installation currently is and show progress during longer stages (i.e. while copying/downloading files).	✅
→ 03. MISLEADING BEHAVIOR		
	All app’s functionalities must correlate with the description mentioned in the installation screens.	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
→ 04. UPDATE		
	Software updater can only update main application (must not install any additional software without user consent).	✅
PROHIBITED		
→ 01. BUNDLING SOFTWARE		
	Software without offer screens	✅ N/A - No bundled software
	Any form of promoting exaggerated or false claims about user system (health, registry, files, etc...).	✅ N/A - No bundled software
→ 02. USER CONSENT, CONTROL AND TRANSPARENCY		
	Sell or otherwise share user personal identifying information to 3rd parties without user explicit consent.	✅
	Any software must have its own privacy policy to describe its data collection, usage and sharing practices.	✅
	Software must not bypass/hack system or other apps security and consent features (browser hijack, disable notification...).	✅
	Software must not operate, access any content or cause use of user's pc without prior informed consent (i.e. operate BitCoin miners).	✅
	Software must not redirect/block/modify searches, queries, user-entered URLs etc. without user consent.	✅
	Software must not access any other site that doesn't directly relate to consented software functionality.	✅
	Any type of installation which does not require the End Users' informed consent is expressly prohibited.	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
→ 03. MISLEADING BEHAVIOR		
	Installer must not mislead a user to take action he has previously declined.	✅
	Revenue modules must not engage with fictional installations of the product or the revenue model.	✅
	All forms of displaying exaggerated/misleading/inaccurate claims about the system's health/files/registry or other items on the system are strictly prohibited.	✅
	Installer must not initiate install of app based on false/misleading/fraud representation.	✅
	Software must not falsely claim to be a program from other brands (Avast, Microsoft, Google, Adobe...).	✅
→ 04. INTERFERING		
	Software must not engage with interfering, replacing, uninstalling or disabling any third party content, application, browser functionality and/or settings, websites, widget, the operating system or any part thereof without user consent.	✅
	Software must not engage in any fraud activity.	✅
	Software must not interfere with browser default search/search pages without the user's consent.	✅

3. PROGRAM FUNCTIONALITY

MUST HAVE

→ 01. TRANSPARENCY AND ATTRIBUTION		
	Ads must include clear attribution to the providing application.	✅ N/A - No advertising
	Ads must be clearly labeled and identified as such.	✅ N/A - No advertising
	When injecting data into external content (such as website, search results..), monetization services must be clearly labeled and identified as distinguished from any content (such as website) it appears on.	✅ N/A - No advertising

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	Ad will carry a link to an "Ad Info" webpage with the following prominent notices and information: a short explanation about why the Ads was displayed, links to the Advertiser's full and clear description of the revenue module, links to the Product's terms of service and privacy policy.	✅ N/A - No advertising
→ 02. PROGRAM BEHAVIOR		
	Once a user uninstalled an app and/or monetization module attributed to that specific app, it must completely remove all components with no remains on the user's PC.	✅
	The uninstall process should function properly and be a mirror of the installation process.	✅
	The installed software must have a corresponding "Add/Remove" entry in Windows Control Panel or equivalent on different platforms, and the user must be able to completely uninstall.	✅
	Software name (as was shown in the installation process and operation of the app and/or monetization module) must be identical to the one in the OS add/remove in control panel.	✅
	Software or the ads attributed to it must have an easy way to close them.	✅
PROHIBITED		
→ 01. TRANSPARENCY AND ATTRIBUTION		
	A program must not fail to clearly indicate when the program is active, and must not attempt to hide or disguise its presence.	✅
→ 02. PROGRAM BEHAVIOR		
	Software must not include monetization services that are Pop-Ups, Pop-Unders, Expanding banners etc.	✅
	Software will not use the end user's device for purposes that are unwarranted and unexpected by the end user.	✅
	Software may not decrease computer reliability and/or cause a poor end user experience.	✅

4. PRIVACY POLICY AND EULA

MUST HAVE

→ 01. PRIVACY POLICY

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	App and/or monetization service's privacy policy shall comply with applicable privacy and data collection and protection laws, and shall provide a clear and comprehensive description of the Advertiser's data collection practices.	✅
	Privacy Policy must describe if software uses cookies or other means of collecting User data.	✅
	Privacy Policy must describe if software accesses, collects, uses, or discloses user's Personally Identifiable Information (PII).	✅
	Privacy Policy must describe what user data is accessed, collected, used, or disclosed, how it is done, and what is done with the data collected.	✅
	Privacy Policy must explain how a user can notify that they wish to opt out from PII collection and have the app and/or monetization service stop collecting PII data about them, and users must be able to achieve this in a straightforward way.	✅

→ 02. EULA

	App and/or monetization service must comply with applicable law, must have EULA that is accessible during the installation process and from the app's website. Vendor and product must comply with the EULA as consented by the user and as was available during installation and on the product.	✅
	App and/or monetization service should be described in a clear EULA. Any material change to the EULA must obtain user consent.	✅

PROHIBITED

→ 01. PRIVACY POLICY

	App and/or monetization service must not sell or otherwise share with third parties personally identifying information without the end user's prior specific consent.	✅
	App and/or monetization service must not mislead users about the origin of cookies and/or other means of data collection, or cause the user to believe it is associated with another app.	✅

Honeygain SDK McAfee compliance report

1. DISTRIBUTION

Objectionable distribution methods can impair the overall user experience. Criteria for evaluating the distribution of software include:

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
PROHIBITED		
	Software must not be linked to or distributed using spam email.	✅
	Software must not be distributed or installed by malware or by otherwise malicious installations (e.g., drive-by).	✅
	Software installers including bundle proxies must not collect or transmit personally identifiable information (PII) without informed user consent.	✅
MUST HAVE		
	Software installers must provide software licensing information prior to the installation of any bundled components.	✅
	Software installers must allow the user to cancel the installation of all components if the installation of any bundled components is required for the main technology.	✅
	Software installers must provide consistent options (e.g., Accept/Decline) when offering bundles. Do not reverse option button order across install windows.	✅
	Any bundled install packages are considered installers and must abide by the same installation notification, consent, and control guidelines as the main installer.	✅

2. DECEPTION

Users must have an informed awareness of software that is installed on their system including the functionality of the software and whether it is active. Criteria for determining deceptive behaviors include:

- **Based on McAfee policy:** media.mcafeeassets.com/content/dam/npcld/ecommerce/en-us/docs/misc/pup-policy.pdf

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
MUST HAVE		
	Information regarding the software publisher, source, website, or identifying information must be reasonable and accurate.	✅
	The legal conditions of the software installation (e.g., software license, EULA) must be clearly indicated in a license agreement.	✅
	Information regarding the software publisher in a Digital Signature must be accurate.	✅
	Software must indicate its behaviors and purpose to give users a meaningful and accurate understanding of the technology.	✅
	Software that tracks user activities (e.g., browsing habits) must not hide, cloak or mislead about this functionality.	✅ Honeygain SDK does not track browsing activity.
	Software uninstall features must adequately remove all functional components of an installation.	✅
	Software must gain informed user consent prior to making or modifying key system settings (Browser plugins, default homepage, search provider, desktop, icons, hosts file, startup registry, security settings).	✅
	Software that makes key system setting changes must reverse these changes during uninstall.	✅
	Additional industry standard criteria may be used to determine deceptive behavior.	✅
PROHIBITED		
	Software must not disguise its presence or masquerade as another technology (e.g., deceptive icons, Version Information, .lnk files).	✅
	Advertisements leading to software downloads must not masquerade as another technology (e.g., fake close buttons).	✅ N/A - No advertising
	Software must not attempt to hide its presence or the presence of other components/software.	✅
	Software must not obfuscate files, filenames, file paths, registry entries beyond reasonable DRM protection.	✅
	Software must not impair the user's ability to uninstall or remove the program.	✅
	Software must not run third-party processes or programs on the system without prior informed user consent.	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	Software must not impair the user's ability to control the software while it runs on the system.	✅
	Software must not install, reinstall, or remove itself or other legitimately installed software without informed user consent/interaction.	✅
	Software must not install other software without clear indication of its relationship to the primary software installation.	✅
	Software cannot use false or misleading endorsements.	✅
	Users must not be misled to believe they have an issue, a problem, something outdated or missing from their system. No exaggerated or unsubstantiated claims about system health.	✅

3. PRIVACY

Users expect that software does not collect, transmit, or reveal sensitive, private information including passwords and personally identifiable information without the express permission of the user or effected individuals. Personally Identifiable Information (PII) is defined differently among jurisdictions. Criteria for determining objectionable behaviors impacting privacy include:

MUST HAVE

	Personally Identifiable Information (PII) definition varies by jurisdiction.	✅
	Includes Name, Address, Phone number, Email, Social Security number, Financial information, etc. (see original policy for full list).	✅
	A user must be able to deactivate software which allows a remote user to access or control the system or send remote commands.	✅
	Software that collects, stores, or transmits user data (including browser activity), passwords, personally identifiable information, or other sensitive information must offer an easily accessible and clear privacy policy.	✅
	Tracking software must provide a runtime notice of its activity.	✅

PROHIBITED

	Software must not reveal, collect, use, or transmit passwords, biometrics, or other credentials without informed user consent of all impacted users.	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	Software must not collect, use, or transmit personally identifiable information (PII) or other sensitive data without informed user consent. PII includes (but is not limited to): – Name – Address – City – State – Postal code/ZIP code – Phone number – Date of Birth – Social Security/tax ID number – Passport number – Driver's license number – Other government-issued identification number – Bank account number or other financial account information (for example, PayPal, Apple Pay, Google Wallet, E*TRADE) – Credit card number – Email address	✅ Honeygain SDK collecting ONLY IP address
	Software must not track user online activities such as web browsing habits, instant messaging chats, or keystrokes without informed user consent.	✅
	Software must not allow user communications to be monitored, redirected, or changed without informed user consent.	✅
	Software must not allow a remote user to access or control the system or send remote commands without informed user consent.	✅
	Software cannot install proxies or redirect network traffic without consent.	✅
	Software must not require additional user information before it can be uninstalled (for example, email address).	✅
	Software must not bypass or facilitate bypassing of other software licensing by using software decipherers or altering another piece of software in such a way that bypasses licensing restrictions.	✅
	Software must not generate license keys for another piece of unrelated software which can facilitate licensing restrictions to be bypassed.	✅

4. SECURITY

Users expect that software does not impede their system security settings, data confidentiality, or the integrity, stability, or availability of their system and its resources. Criteria for determining objectionable behaviors impacting security include:

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
MUST HAVE		
	Software that requires elevated privileges to execute or that facilitates another application to run with elevated privileges must prompt the user to enter credentials for the elevated user with informed notification of the need to do so.	✅
PROHIBITED		
	Software must not attempt to evade security features of the system or installed security products (this does not include reasonable DRM protection such as runtime packers, encryptors, etc.).	✅
	Software must not attempt to disable or bypass security features of the system or installed security products without informed consent of the user.	✅
	Software must not change settings of the operating system, security software, or other unrelated software without informed consent of the user..	✅
	Software must not exploit software or system vulnerabilities.	✅
	Software must not facilitate a denial of service (that is, DOS or DDOS) against an application, system or network through exploit, flooding with network traffic or by any other means.	✅

5. ADVERTISING

Unexpected advertisements can be a deception to the user. For the purposes of this document, advertising methods may include software which creates pop-ups, pop-unders, slide-ins, or inserts advertisements into the context of a web page. Criteria for determining objectionable advertising behaviors include:

MUST HAVE		
	Advertising methods include pop-ups, pop-unders, slide-ins, or insertions into web pages.	✅ N/A - No advertising
	Advertisement content/logos must direct users to relevant content.	✅ N/A - No advertising

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	Advertisements must be clearly labeled with the source program/ technology/product.	✅ N/A - No advertising
PROHIBITED		
	Software must not provide pop-up, pop-under, or slide-in advertisements without informed user consent.	✅ N/A - No advertising
	Advertisements must not be false, fraudulent, deceptive, misleading, vulgar, pornographic, or offensive.	✅ N/A - No advertising
	Pop-up advertisements must not impair the user's ability to close them or control the system/software.	✅ N/A - No advertising
	Closing one pop-up must not create additional pop-up windows.	✅ N/A - No advertising
	Software must not replace advertisements of other legitimate sites without user consent.	✅ N/A - No advertising
	Software must not insert advertisements into the content of another application.	✅ N/A - No advertising

6. PERFORMANCE, STABILITY, AND USER EXPERIENCE

Users expect that the installation of a piece of software does not severely impact the performance or usability of their system or other software. Additionally, negative side effects or features of the software may adversely impact the user experience including annoying advertisements, impairment of system or resource usability, and other drains on the system. Users may expect certain speed impacts for come technologies (for example, security, file sharing products). However, unexpected impairments may cause frustrations or indicate other unexpected problems. Criteria for determining objectionable impacts to system performance, stability, or the user experience include:

	Software must not negatively impact system performance, reliability, or the user experience beyond a reasonable level necessary to provide the functionality agreed to by the user.	✅
	Software must not place a high drain on system resources that result in noticeably slower computer performance without informed user consent.	✅
	Software must not consume large amounts of bandwidth of an internet connection beyond what is reasonable for the type of technology (that is, P2P, online gaming applications, etc.) without informed user consent.	✅
	Software must not negatively impact system reliability without informed user consent.	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	Software must not corrupt the operating system, material components of the system, or other installed software without informed user consent.	✅

7. NOTIFICATION

Central to the evaluation of software risk is the notion that users must be notified of the software installation and the risks associated with it. Notification can occur using many methods and may differ from technology to technology.
Notification may address specific risk behaviors in the software and may alert users to the risks or changes the software will make. Notification may also provide identification of the software so that the user can trace its origin. Notification must be provided for all identified risk behaviors. General notification features may include, but are not limited to:

	Easily accessible and germane End User License Agreement information provided prior to any application installation or collection or transmission of data to a third party	✅
	Valid and germane digital signatures of binary files identifying the vendor, distributor, or manufacturer of the software	✅
	Installation windows that offer users an opportunity to select or deselect unwanted options prior to installation or making system modifications	✅
	Product information in the Resource (.RSRC) Version Information section of Windows binary executable and DLL files that is valid and germane to the vendor, distributor, or manufacturer of the software	✅
	For command-line tools, accurate product name and version information	✅
	For command-line tools, accurate and complete Help information	✅
	For graphical user interfaces, germane product identification in main windows, window frames, or “About” window	✅
	Installation paths that include accurate names germane to the installation	✅
	Filenames that are not randomized to obfuscate or otherwise mask the technology	✅
	Files and components that are not obfuscated beyond any reasonable DRM protection	✅
	Embedded Windows binary icons (embedded in PE file RSRC section) that accurately represent the technology	✅
	Files or content that are not padded with data that impairs the user’s ability to accurately identify the technology, vendor, distributor, or manufacturer	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	For pop-up windows or advertisements, identification in the window frame that indicates the application generating the pop-up	✅ N/A - no pop-up / advertisements
	Startup menu items that clearly identify the application	✅
	Desktop shortcut names that are germane to the installation	✅ N/A - no desktop shortcuts
	Desktop shortcut icons that are germane to the installation	✅ N/A - no desktop shortcuts
	Windows registry key entries that are not obfuscated in a manner that hides the identity of the technology beyond reasonable DRM measures	✅
	For tracking (for example, keylogger or spyware) software that monitors user online activities, notification that the software is running or active, and is easily visible to all affected users prior to any data or activity collection (for example, login notice, runtime system tray icon, pop-up alert, or warning before any monitoring takes place, etc.)	✅ Honeygain SDK does not monitor or track users' online activities.
	For bundled applications, notification of bundled components prior to their installation	✅ N/A - No bundled software
	For software updates, clear indication that the software or components are being updated or that an update is available	✅
	For Uninstall entries in the system Add/Remove Programs interface, clear identification for the technology	✅
	For Uninstall entries in the Startup menu, clear identification for the technology	✅

8.CONSENT

Software must obtain informed consent of the user to any risks posed by the software prior to the actions of the software. Consent may be obtained through several acceptable means including:

Consent can be obtained through software distribution websites.	✅
Consent can be obtained through software license agreements.	✅
Consent can be obtained through software/website privacy policies.	✅
Consent can be obtained through software installation menus (including license/privacy info).	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	Consent can be obtained through runtime alerts/notifications (including uninstall consent).	✅

9. CONTROL

Users should be able to control the installation process of an application or installation and have fundamental control over the technology once installed including starting and stopping the application. Additionally, a user should be able to adequately uninstall or remove the application from a system once its use is no longer desired. A user should be able to see that a program is running on their system. This can include system tray icons, entries in browser add-on management interfaces, task manger entries, etc. Users must also be aware if a program updates itself or its components. Users must also be in control of their personal information and the use or transmission thereof.

MUST HAVE

	Software that is configured to automatically load at system startup or user login must provide a clear mechanism to disable, adequately adjust this setting, or totally remove the software.	✅ N/A - defined by the SDK carrier
	Software that is not standalone (that is, a command-line tool or standalone program/component) must provide a clear uninstall mechanism. Uninstall options may be found in several locations, including Add/Remove Programs, Windows Start Menu Uninstall feature, Windows System Tray, or menu items within the software user interface.	✅ N/A - defined by the SDK carrier
	Software that is standalone (that is, a command-line tool or single-click app) must be able to be removed through standard file delete functionality.	✅ N/A - defined by the SDK carrier
	Software must inform the user if updates are to be downloaded or installed automatically.	✅
	Software that tracks a user's online activities must be easily deactivated or uninstalled.	✅

Honeygain SDK Microsoft compliance report

1. UNWANTED SOFTWARE

Microsoft believes that you should have control over your Windows experience. Software running on Windows should keep you in control of your device through informed choices and accessible controls. Microsoft identifies software behaviors that ensure you stay in control. We classify software that doesn't fully demonstrate these behaviors as ""unwanted software".

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
PROHIBITED		
→ 01. LACK OF CHOICE		
	Fail to clearly indicate when the software is active. It might also attempt to hide or disguise its presence.	✅
	Install, reinstall, or remove software without your permission, interaction, or consent.	✅
	Install other software without a clear indication of its relationship to the primary software.	✅
	Circumvent user consent dialogs from the browser or operating system.	✅
	Falsely claim to be software from Microsoft.	✅
	Display exaggerated claims about your device's health.	✅
	Make misleading or inaccurate claims about files, registry entries, or other items on your device.	✅
	Display claims in an alarming manner about your device's health and require payment or certain actions in exchange for fixing the purported issues.	✅
MUST HAVE		
	Give you notice and get consent to do so. Software shouldn't include an option that configures it to hide activities associated with storing or transmitting your data.	✅

• **Based on Microsoft criteria:** https://learn.microsoft.com/en-us/unified-secops/criteria

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
PROHIBITED → 02. LACK OF CONTROL	Prevent or limit you from viewing or modifying browser features or settings.	✅
	Open browser windows without authorization.	✅
	Redirect web traffic without giving notice and getting consent.	✅
	Modify or manipulate webpage content without your consent.	✅
PROHIBITED → 03. INSTALLATION AND REMOVAL	Present confusing or misleading prompts or pop-ups when you try to uninstall it.	✅
	Fail to use standard install/uninstall features, such as Add/Remove Programs.	✅
MUST HAVE → 04. ADVERTISING AND ADVERTISEMENTS	The advertisements that are presented by software must include an obvious way for users to close the advertisement. The act of closing the advertisement must not open another advertisement.	✅ N/A - No advertising
	The advertisements that are presented by software must include the name of the software that presented the advertisement.	✅ N/A - No advertising
	The software that presents these advertisements must provide a standard uninstall method for the software using the same name as shown in the advertisement it presents.	✅ N/A - No advertising

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	Advertisements shown to you must be distinguishable from website content.	✅ N/A - No advertising
	Advertisements shown to you must not mislead, deceive, or confuse.	✅ N/A - No advertising
	Advertisements shown to you must not contain malicious code.	✅ N/A - No advertising
	Advertisements shown to you must not invoke a file download.	✅ N/A - No advertising

2. POTENTIALLY UNWANTED APPLICATION (PUA)

"PUAs aren't considered malware.
Microsoft uses specific categories and the category definitions to classify software as a PUA."

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
PROHIBITED	Advertising software: Software that displays advertisements or promotions, or prompts you to complete surveys for other products or services in software other than itself. This includes software that inserts advertisements to webpages.	✅ N/A - No advertising
	Torrent software (Enterprise only): Software that is used to create or download torrents or other files specifically used with peer-to-peer file-sharing technologies.	✅ N/A - Not a torrent software
	Cryptomining software (Enterprise only): Software that uses your device resources to mine cryptocurrencies.	✅ N/A - Not a cryptomining software
	Bundling software: Software that offers to install other software that is not developed by the same entity or not required for the software to run. Also, software that offers to install other software that qualifies as PUA based on the criteria outlined in this document.	✅ N/A - No bundled software
	Marketing software: Software that monitors and transmits the activities of users to applications or services other than itself for marketing research.	✅ N/A - Not a marketing software
	Evasion software: Software that actively tries to evade detection by security products, including software that behaves differently in the presence of security products.	✅ N/A - Not an evasion software
	Poor industry reputation: Software that trusted security providers detect with their security products. The security industry is dedicated to protecting customers and improving their experiences. Microsoft and other organizations in the security industry continuously exchange knowledge about files we have analyzed to provide users with the best possible protection.	✅

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE

3. TAMPERING SOFTWARE

Tampering software encompasses a broad spectrum of tools and threats that directly or indirectly lower the overall level of security of devices.

PROHIBITED

Disabling or uninstalling security software: Tools and threats that attempt to evade defense mechanisms by disabling or uninstalling security software, such as antivirus, EDR, or network protection systems. These actions leave the system vulnerable to further attacks.	✅ N/A - Not a tampering software
Abusing operating system features and settings: Tools and threats that exploit features and settings within the operating system to compromise security. Examples include: - Firewall abuse: Attackers using firewall components to indirectly tamper with security software or block legitimate network connections, potentially enabling unauthorized access or data exfiltration. - DNS manipulation: Tampering with DNS settings to redirect traffic or block security updates, leaving the system exposed to malicious activities. - Safe mode exploitation: Leveraging the legitimate Safe Mode setting to put the device in a state where security solutions might be bypassed, allowing for unauthorized access or malware execution.	✅ N/A - Not a tampering software
Manipulating system components: Tools and threats that target critical system components, such as kernel drivers or system services, to compromise the overall security and stability of the device.	✅ N/A - Not a tampering software
Privilege escalation: Techniques aimed at elevating user privileges to gain control over the system's resources and potentially manipulate security settings.	✅ N/A - Not a tampering software
Interfering with security updates: Attempts to block or manipulate security updates, leaving the system vulnerable to known vulnerabilities.	✅ N/A - Not a tampering software
Disrupting critical services: Actions that disrupt essential system services or processes, potentially causing system instability and opening the door for other attacks.	✅ N/A - Not a tampering software
Unauthorized registry changes: Modifications to the Windows Registry or system settings that impact the security posture of the device.	✅ N/A - Not a tampering software
Tampering with boot processes: Efforts to manipulate the boot process, which can result in the loading of malicious code during startup.	✅ N/A - Not a tampering software

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE

4. MALICIOUS SOFTWARE

Malicious software is an application or code that compromises user security. Malicious software could steal your personal information, lock your device until you pay a ransom, use your device to send spam, or download other malicious software. In general, malicious software wants to trick, cheat, or defrauds users, placing them in vulnerable states.

PROHIBITED

Backdoor: A type of malware that gives malicious hackers remote access to and control of your device.	✅ N/A - Not a malware
Command and Control: A type of malware that infects your device and establishes communication with the hackers' command-and-control server to receive instructions. Once communication is established, hackers can send commands that can steal data, shut down and reboot the device, and disrupt web services.	✅ N/A - Not a malware
Downloader: A type of malware that downloads other malware onto your device. It must connect to the internet to download files.	✅ N/A - Not a malware
Dropper: A type of malware that installs other malware files onto your device. Unlike a downloader, a dropper doesn't have to connect to the internet to drop malicious files. The dropped files are typically embedded in the dropper itself.	✅ N/A - Not a malware
Exploit: A piece of code that uses software vulnerabilities to gain access to your device and perform other tasks, such as installing malware.	✅ N/A - Not a malware
Hacktool: A type of tool that can be used to gain unauthorized access to your device.	✅ N/A - Not a malware
Macro virus: A type of malware that spreads through infected documents, such as Microsoft Word or Excel documents. The virus is run when you open an infected document.	✅ N/A - Not a malware
Obfuscator: A type of malware that hides its code and purpose, making it more difficult for security software to detect or remove.	✅ N/A - Not a malware
Password stealer: A type of malware that gathers your personal information, such as usernames and passwords. It often works along with a key logger, which collects and sends information about the keys you press and websites you visit.	✅ N/A - Not a malware
Ransomware: A type of malware that encrypts your files or makes other modifications that can prevent you from using your device. It then displays a ransom note that states you must pay money or perform other actions before you can use your device again.	✅ N/A - Not a malware
Rogue security software: Malware that pretends to be security software but doesn't provide any protection. This type of malware usually displays alerts about nonexistent threats on your device. It also tries to convince you to pay for its services.	✅ N/A - Not a malware

CATEGORY	FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
	Trojan: A type of malware that attempts to appear harmless. Unlike a virus or a worm, a trojan doesn't spread by itself. Instead, it tries to look legitimate to trick users into downloading and installing it. Once installed, trojans perform various malicious activities such as stealing personal information, downloading other malware, or giving attackers access to your device.	✅ N/A - Not a malware
	Trojan clicker: A type of trojan that automatically clicks buttons or similar controls on websites or applications. Attackers can use this trojan to click on online advertisements. These clicks can skew online polls or other tracking systems and can even install applications on your device.	✅ N/A - Not a malware
	Worm: A type of malware that spreads to other devices. Worms can spread through email, instant messaging, file sharing platforms, social networks, network shares, and removable drives. Sophisticated worms take advantage of software vulnerabilities to propagate.	✅ N/A - Not a malware

Honeygain SDK Malwarebytes compliance report

PUP CRITERIA

FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
Identifying potentially unwanted software is complex due to rapid evolution and masking of unwanted functions.	✅
Identifying common behaviors is an ongoing process for maximum protection.	✅
Norton uses judgement in cases of questionable behavior, even if it doesn't perfectly align with criteria.	✅
Users control what to keep or remove via the exclusions list.	✅
Obtrusive, misleading, or deceptive advertising, branding, or search practices.	✅
Using pop-ups, pop-unders, ad-insertion, ad-overlays, or ad replacement.	✅ N/A - No advertising
Excessive/deceptive distribution practices, affiliate bundling, or SEO poisoning.	✅
Aggressive/deceptive behavior surrounding purchasing/licensing.	✅
Unwarranted/excessive modifications to system/security settings.	✅
Using fake installers (e.g., Adobe Flash Player) to push products.	✅
Using exaggerated findings to scare users into purchasing.	✅
Using technical support scam tactics.	✅
Difficulty uninstalling or removing the software.	✅
Predominantly negative feedback/ratings from the user community.	✅
Generally hurting or diminishing end-user experience.	✅
Practices generally accepted as riskware, scareware, adware, or greyware.	✅
Identifying potentially unwanted software is complex due to rapid evolution and masking of unwanted functions.	✅
Identifying common behaviors is an ongoing process for maximum protection.	✅

- **Based on Malwarebytes criteria:** www.malwarebytes.com/pup

Honeygain SDK Google compliance report

1.GENERAL

FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
Focus on providing a great user experience.	✅
Software should not be deceptive, tricking users or failing to meet promises.	✅
Software must disclose all principal and significant functions.	✅
Software should not have unexpected impacts on the system.	✅
Software should be easy to remove.	✅
Software must not collect/transmit private info without user knowledge.	✅ Honeygain SDK collecting ONLY IP address
Bundled software must be disclosed.	✅ N/A - No bundled software

2. TRANSPARENT INSTALLATION AND UPFRONT DISCLOSURE

The software installation process should be straightforward, easy-to-understand and based on clear choices made by the user. It should present a clear value proposition to the user.

Programs should have a valid and verified code signature issued by a code-signing authority that presents verifiable publisher information.	✅
Download of the software should only begin when the user has consented to the download by clicking on a clearly-labelled download button.	✅
At the time of installation, all principal and significant functions of the software should be described in clear and straightforward language that is clearly visible and easy to read on the screen.	✅

• **Based on Google criteria:** www.google.com/about/unwanted-software-policy.html

FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
The user must have a meaningful opportunity to review and approve all principal and significant proposed installation options and system changes. For example, at the time of installation, the software might list each of the proposed settings changes, and note that the programme collects the user's personal data, with links to learn more about each of the changes.	✅
As part of the install flow, any bundled software must be clearly disclosed. No software should be installed silently without the user's permission. The name and principal and significant functions of every piece of software that will be installed should be visible to the user, and the user should be able to skip the entire bundled software or offer as well as individual components of the bundle.	✅
Before and during the install process, the software must not engage in any deceptive behaviours. Some examples of deceptive behaviours include: - Making false or misleading claims about the state of the user's system. For example, misleading claims related to antivirus protection, system performance, system optimisation, a new version of a plug-in, etc. - Claiming or implying to be official software from a company or a partner of the company if that is not the case. - Charging fees for software that is available elsewhere for free without disclosing this to the user and explaining what extra service justifies the fee. - Providing unproven or misleading endorsements.	✅
The software and download page must contain a link to an End User Licence Agreement (EULA) or Terms of Service (TOS).	✅

3. REMOVAL

It should be easy for users to disable or uninstall software.

Uninstall information must be easily accessible, simple to perform, and clearly identifiable after the software has been installed.	✅
During the uninstall process, users must be presented with clearly-labelled and prominent instructions that explain how to return their browser's and/or computer's user settings to the previous settings.	✅
The software must provide a clear uninstall process and must not engage in any deceptive behaviours to deter uninstallation. Some examples of deceptive behaviours include: - Making false or misleading claims about potential negative effects on the user's system or privacy if the software is uninstalled. - Charging fees for software removal. - Including additional prompts or offers that are unnecessary to the uninstall process. - Making the default option in the uninstaller to hide the software instead of removing it.	✅

FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
Uninstallation must not impact unrelated files.	✅
Once software is disabled or deleted, the removal should be complete. Configuration changes that affected the behaviour of already existing software should be reverted. It may not keep any pieces of the software running after uninstallation and must not be automatically enabled later by itself or another programme.	✅

4. CLEAR BEHAVIOR

Once installed, software should behave as expected and deliver a clear value proposition to the user.

After installation, the program should not download or install additional software, or make system settings changes, beyond what was offered during the initial installation, unless it is doing so at the explicit, informed direction of the user.	✅
When accessing Google services or products, software must use and adhere to the terms of publicly-available Google APIs for interacting with the user's system or any program installed. In addition, software must comply with any other applicable Google policies.	✅
After installation, programs should not engage in deceptive or unexpected behaviour. Some examples of deceptive or unexpected behaviour include: - Displaying false or misleading messages about the system status. Hiding or cloaking the software's behaviour. Behaving differently when running in a virtualised environment. - Impairing usability of the system. Remapping inputs, unless the program is doing so at the explicit, informed direction of the user. - Preventing the user from controlling the software, or interfering with control of, or access to, any other program already installed on the system. - Affecting the integrity of other programs, including disabling or circumventing security and protection measures, unless the program is doing so at the explicit, informed direction of the user. - Intercepting and redirecting network traffic, unless it is the stated purpose of the software.	✅
The software should not send spam. It should not inject ads, unless that is the stated purpose of the program.	✅
If the software makes updates, it should provide a clear notification to the user. The user must have a meaningful opportunity to review and approve any principal and significant updates or settings changes.	✅

FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE

5. SNOOPING

Software that collects or transmits a user's personal information must be transparent about doing so.

Software that collects and/or transmits users' personal information must be transparent about it by providing an explanation in clear and straightforward language that describes what information would be collected or transmitted and for what purpose. The language should be clearly visible and easy to read on the screen. Disclosure is especially important if data collection is a non-obvious feature of the software.	✅
Software must not collect sensitive information such as banking details without proper encryption.	✅

6. BUNDLING

If any program includes any third-party software, the author is responsible for obtaining proper bundling authorisation from the third party.	✅ N/A - No bundled software
If software is offered as part of a bundle, all programs included in the bundle must follow the guidelines above.	✅ N/A - No bundled software

Honeygain SDK Avira compliance report

1. DEFAULT INSTALLATION FLOW / THIRD PARTY SOFTWARE

FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
Following the software's default installation flow, are there any undesired software installations or changes to the system (such as changes to files, to the registry, to settings, etc.) that are unrelated to the software intended to be installed by the user?	✅
Does the software install third party software and/or unrelated components without explicit user consent?	✅
Does the software manipulate the user via social engineering to install unrelated components or additional software?	✅

2. UNINSTALLATION

Are any of the software components hidden or cannot be uninstalled by normal user means?	✅

3. PUBLISHER INFORMATION

Does the software contain incorrect and/or incomplete details regarding brand ownership or license? Are any digital certificates used invalid? Does your software fail to display an End User License Agreement (EULA)?	✅

4. SOFTWARE DESCRIPTION MISSING / MISLEADING

Is the software description missing or does it, at any point, misrepresent the software's actual functionality?	✅

- **Based on Avira guidelines:** https://www.avira.com/en/potentially-unwanted-applications

FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
5. MANDATORY OFFERS	
Does the installation flow of the software claim that it is mandatory to agree or accept additional offers in order to complete the installation process successfully?	✅
6. MALICIOUS COMPONENTS	
Is the software bundled with malicious or potentially unwanted content?	✅
7. CHANGING BROWSER SETTINGS / BEHAVIOR	
Does the installation flow of the software change any user settings, default settings (for example, default search engine, default homepage, default browser, bookmarks) or profiles without the user's explicit consent?	✅
8. MISLEADING CLAIMS	
Does the software show misleading or exaggerated claims? Does it trick the user into thinking their computer has problems that it does not have?	✅
9. PERMISSIONS	
Does the software request permissions that are unnecessary for it to complete its promoted purpose?	✅

FULL REQUIREMENT DESCRIPTION	HONEYGAIN SDK COMPLIANCE
10. COMMUNICATION	
Does the software use the user's identity to send or post content, or use the user's identity in any other manner, without the clear consent of the user?	✅
11. THREATENING OR SCARY MESSAGES	
Does the software attempt to threaten or scare the user into taking action?	✅
12. PROMOTION OR DISTRIBUTION OF PUA APPLICATIONS	
Does the website promote or provide files to the user that are malicious or potentially unwanted?	✅
13. TRANSPARENCY	
Does the product or its installer avoid investigation or detection, act differently in the presence of anti-malware software/anti-malware environments or virtual machine environments?	✅

The end

honeygain® {dev}